

Notice of Allowability	Application No.	Applicant(s)	
	10/056,060	VANSTONE ET AL.	
	Examiner	Art Unit	
	Jung W. Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 27 October 2005.
2. ☒ The allowed claim(s) is/are 31,33-35,37-39,41,43,45-47.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|---|--|
| 1. <input type="checkbox"/> Notice of References Cited (PTO-892) | 5. <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 6. <input type="checkbox"/> Interview Summary (PTO-413),
Paper No./Mail Date _____. |
| 3. <input type="checkbox"/> Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____ | 7. <input checked="" type="checkbox"/> Examiner's Amendment/Comment |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit
of Biological Material | 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| | 9. <input type="checkbox"/> Other _____. |

DETAILED ACTION

1. This Office action is in response to the amendment filed on October 27, 2005.
2. Claims 31, 33-35, 37-39, 41, 43 and 45-47 are pending.
3. Claims 31, 33, 34, 37, 38, 41, 43, 45 and 46 are amended.
4. Claims 1-30, 32, 36, 40, 42, 44 and 48 are canceled.

Response to Amendment

5. The amendments to the independent claims 31 and 41 incorporate the subject matter of claims 40 and 48 respectively. As indicated in the previous Office action, the prior art of record do not teach this limitation. Hence, claims 31, 33-35, 37-39, 41, 43 and 45-47 are allowed.

Examiner's Amendment

6. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.
7. Authorization for this examiner's amendment was given in a telephone interview with Ralph A. Dowell on November 22, 2005.
8. The application has been amended as follows:

a. In the Specification:

i. Page 3;

(1) Line 18, replace "Figure 3 is a schematic flow chart of an alternative protocol; and" with –Figure 3 is a schematic flow chart of an alternative protocol;--;

(2) Line 19, replace "Figure 4 is a schematic flow chart of a further protocol" with –Figure 4 is a schematic flow chart of a further protocol; and--;

(3) After line 19 and before line 20, add –Figure 5 is a schematic flow chart of a further protocol.--.

Allowable Subject Matter

9. The following is an examiner's statement of reasons for allowance: Applicant's claimed invention is directed to a method of establishing a session key between a pair of correspondents, wherein secret information is shared and additional secret information is generated to further derive a session key. The prior art of record teaches a similar invention. However, the prior art does not teach the limitation of generating a first signature component using the additional secret information and generating a second signature component using the secret information, wherein the second signature component is verified by operating on the session key to obtain a value corresponding to the second signature component and comparing the value with the second signature component. Hence, 31, 33-35, 37-39, 41, 43 and 45-47 are allowed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Communications Inquiry


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

November 16, 2005


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100